REMARKS

Applicants have amended claims 1-14, 16, and 17. Applicants respectfully submit that no new matter is being added by these amendments.

Rejection Under 35 U.S.C. § 102

The Examiner rejected claims 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 18, and 20 under 35 U.S.C. § 102(e) as being anticipated by Bialick. Applicants respectfully traverse.

Claim 1 recites that "access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise." Bialick does not teach or disclose this limitation.

In paragraph 4 of the Office Action, the Examiner cited col. 10:45-11:10 of Bialick as teaching that an access code, such as a PIN, password, or biometrics, has to be entered before a user is enabled to access data stored in a memory of a peripheral device. As will be explained below, the Examiner's reliance on this portion of Bialick is misplaced as it does not disclose that an access code entered via a biometrics-based device can enable access to data stored in a memory of the peripheral device.

Column 10:45-11:10 of Bialick states:

The peripheral device driver can be implemented so that the user must successfully enter an acceptable access code (e.g., a password or PIN) before the user is enabled to use the peripheral device. In particular, it can be desirable to require an access code before enabling a user to use the security functionality, thus establishing a layer of security that protects the integrity of the security operations themselves. In the method **700**, as shown by the step **704**, an acceptable access code must be entered by the user before the security functionality of the peripheral device can be used. An access code can be entered, for example, by inputting the access code in a conventional manner using a user interface device (e.g., keyboard) of the host computing device. Or, an access code can be entered using particular embodiments of target functionality (such as a biometric device, discussed in more detail below) that is part of the peripheral device according to the invention.

Advantageously, an access code can be used not only to control access to the security (or other) functionality of the peripheral device, but also to identify a "personality" of the user. Each personality is represented by data that establishes certain characteristics of operation of the peripheral device, such as, for example, restrictions on operation of the peripheral device (e.g., limitations on the types of security operations that can be performed) or specification of operating parameters or characteristics (e.g., cryptographic keys or specification of a particular incarnation of a type of security algorithm, such as a particular encryption algorithm). A single user can have multiple personalities: each personality might, for example, correspond to a different capacity in which a user acts. Data representing personalities and corresponding user access codes can be stored in a memory device of the peripheral device.

This portion of Bialick does not disclose that an access code is required before a user is enabled to access data stored in a memory of a peripheral device. Bialick discloses that "it can be desirable to require an access code before enabling a user to use the security functionality" of the peripheral device (col. 10:48-50, emphasis added), and that "an

acceptable access code must be entered by the user before the security functionality of the peripheral device can be used" (col. 10:53-55). Further, Bialick identifies storing data as a target functionality: "referred to herein as 'target functionality'. . . such as, for example, the capability to store data in a solid-state disk storage device" (col. 4:64-66). Bialick discloses that entering an access code using a biometrics device is also a target functionality (col. 10:58-60; col. 14:49-50). Bialick does not teach that storing data in a memory of the peripheral device is a security functionality.

Bialick discloses a peripheral device having only two functionalities: (1) a security functionality and (2) a target functionality (col. 4:55-65). Bialick defines a security functionality as "operations that provide one or more of the basic cryptographic functions, such as maintenance of data confidentiality, verification of data integrity, user authentication and user non-repudiation" (col. 5:22-28). Bialick identifies the following as examples of a security functionality: cryptographic key exchange operations (col. 18:1-3); hash operations (col. 18:7-8); digital signature operations (col. 18:12-13); key wrapping operations for symmetric and asymmetric keys (col. 18:17-19); symmetric encryption operations (col. 18:23-24); asymmetric (public key) encryption operations (col. 18:28-30); and exponentiation operations (col. 18:37-39). These examples of security functionalities all relate to performing some type of encryption on data. None of the disclosed examples of a security functionality is storing data in a non-volatile memory of a portable device, and storing data in a non-volatile memory of a portable device is not a cryptographic function.

Bialick does not disclose an embodiment or mode of operation of the peripheral device in which two different target functionalities are used. Bialick discloses three modes that the invention can be operated in: a mode in which only the security functionality is used,

a mode in which both the security functionality and the target functionality are used, and a mode in which only the target functionality is used. *See* col. 10:13-18; col. 11:29-30; col. 3:36-40. Bialick does not disclose a mode in which more than one target functionality is used. When the target functionality is embodied as a biometric device, the "transaction" of the peripheral device is a security functionality. *See* col. 12:24-33; FIG. 7 (steps 714 & 715). While Bialick states that "an access code can be used not only to control access to the security (or other) functionality of the peripheral device" (col. 10:62-64), Applicants respectfully submit that the presence of the two words "or other" is not a sufficient disclosure to inform one of ordinary skill in the art that Bialick discloses an embodiment or mode of operation of the peripheral device with more than one target functionality.

Thus, the portion of Bialick relied upon by the Examiner fails to teach or disclose "access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise" as recited in claim 1.

Bialick does not disclose all of the limitations of claim 1. Thus claim 1 is not anticipated by Bialick and is in condition for allowance.

Claim 7 recites that the microprocessor is configured to "determine whether the second biometrics marker can be authenticated against the first biometrics marker; and . . . to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module" As set forth above regarding claim 1, Bialick does not disclose that the peripheral device can operate in a mode of operation in which more than one target functionality can be used. Bialick does not disclose that entering an access code using a

biometrics device, which is a target functionality, enables a user to access a memory of the peripheral device, where storing data is another target functionality.

Bialick does not disclose all of the limitations of claim 7. Thus claim 7 is not anticipated by Bialick and is in condition for allowance.

Claim 17 recites "comparing the first biometrics marker against the registered biometrics marker" and "denying the user access to the non-volatile memory provided that a match is not identified." Bialick does not disclose that access to a non-volatile memory of the peripheral device is denied if a match against a registered biometrics marker is not identified. As set forth above regarding claim 1, Bialick does not disclose that the peripheral device can operate in a mode of operation in which more than one target functionality can be used. Bialick does not disclose that entering an access code using a biometrics device, which is a target functionality, enables a user to access a memory of the peripheral device, where storing data is another target functionality.

Claims 2, 4, 5, 8, 10, 11, 13, 14, 18, and 20 depend from one of independent claims 1, 7 and 17, and are therefore allowable for at least the same reasons.

Rejection Under 35 U.S.C. § 103

The Examiner rejected claims 6, 12, 16, 19 and 22 under 35 U.S.C. § 103(a) as being unpatentable over Bialick. Applicants respectfully traverse.

Claims 6, 12, 16, 19, and 22 depend from one of claims 1, 7, and 17, and are therefore allowable for at least the same reasons.

Claims 6 and 16 recite that the "microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module." Bialick does not disclose a microprocessor that

provides a bypass mechanism for authentication when authentication by a biometrics-based authentication module fails. The cryptographic processing device 801 of Bialick is not configured to provide a bypass mechanism for authentication. The Examiner has not identified any prior art reference that discloses a microprocessor that provides a bypass mechanism for authentication when a biometrics-based authentication fails.

The Examiner stated that it would have been obvious to modify Bialick to include a microprocessor configured to provide a bypass mechanism because "a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by [Bialick] to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources." Applicants respectfully disagree. Simply suggesting use of a security functionality does not teach or suggest use of a bypass mechanism for authentication when a biometrics-based authentication module fails. Applicants' specification identifies an example of a situation in which the claimed bypass mechanism can be used: a malfunction of verification module 12b. In the event of a biometrics-based authentication module malfunction, the bypass mechanism can enable an authorized user to gain access to the data stored in the memory of the portable device until the module is repaired. *See* specification, pp. 13-14. Bialick identifies no such situation, and does not teach or suggest that there is any need to deal with a malfunction of a biometrics-based authentication. Bialick does not teach or suggest using an additional user authentication mechanism when a biometrics-based authentication fails. Thus claims 6 and 16 are not obvious in view of Bialick and are in condition for allowance.

Claim 22 recites a step of "providing the user with a bypass authentication procedure provided that a match is not identified." The Examiner stated that it would have been obvious

to modify Bialick to include a step of providing a bypass authentication procedure provided that a match is not identified because "a person having ordinary skill in the art would have been motivated to do so by the suggestion provided by [Bialick] to use the security functionality, thus enabling a layer of security that protects the integrity of the restricted resources." Applicants respectfully disagree. Simply suggesting use of a security functionality does not teach or suggest use of a bypass authentication when a match between biometrics markers is not identified. Applicants' specification identifies an example of a situation in which the claimed bypass mechanism can be used: a malfunction of verification module 12b. In the event of a biometrics-based authentication module malfunction, the bypass mechanism can enable an authorized user to gain access to the data stored in the memory of the portable device until the module is repaired. *See* specification, pp. 13-14. Bialick identifies no such situation, and does not teach or suggest that there is any need to deal with a failure of a biometrics-based authentication. There is no teaching or suggestion in Bialick of using an additional authentication procedure when a match between biometrics markers is not identified. Thus claim 22 is not obvious in view of Bialick and is in condition for allowance.

Claim 12 recites that "the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory." The Examiner stated that it would have been obvious to one of ordinary skill in the art to modify Bialick to include encrypting a first biometrics marker before storing the first biometrics marker in a non-volatile memory, and that Bialick provides a suggestion to enhance the security of a biometrics-based access control method. Applicants respectfully disagree. Bialick does not teach or suggest performing any type of security functionality,

such as a cryptographic operation, on a biometrics marker that is to be stored in a non-volatile memory of a peripheral device. Bialick teaches that a cryptographic operation is a security functionality that is separate from any target functionality. There is no teaching or suggestion in Bialick to modify a biometrics-based authentication to encrypt a first biometrics marker before storing the first biometrics marker in the non-volatile memory of a portable device. Thus claim 12 is not obvious in view of Bialick and is in condition for allowance.

Claim 19 recites that "the registered biometrics marker is stored in an encrypted format." The Examiner stated that it would have been obvious to one of ordinary skill in the art to modify Bialick to include storing a registered biometrics marker in an encrypted format, and that Bialick provides a suggestion to enhance the security of a biometrics-based access control method. Applicants respectfully disagree. Bialick does not teach or suggest performing any type of security function, such as a cryptographic operation, on a registered biometrics marker that is stored in a non-volatile memory of a peripheral device. Bialick teaches that a cryptographic operation is a security functionality that is separate from any target functionality. There is no teaching or suggestion in Bialick to modify a target functionality of biometrics-based authentication to store a registered biometrics marker in an encrypted format. Thus claim 19 is not obvious in view of Bialick and is in condition for allowance.

The Examiner rejected claims 3 and 9 under 35 U.S.C. § 103(a) as being unpatentable over Bialick in view of Bjorn. Applicants respectfully traverse.

Claims 3 and 9 depend from claims 1 and 7, respectively, and are therefore allowable for at least the same reasons. Further, claims 3 and 9 are allowable over Bialick in view of

Bjorn because these references, either alone or in combination, do not teach or disclose all the limitations of claims 3 and 9.

Claim 3 recites a "USB plug for coupling the portable data storage device directly to a USB socket of another USB-compliant device." The Examiner stated that Bialick does not disclose this limitation, but that Bjorn teaches a device with a data bus that conforms to a USB standard (col. 2:59-60) and that it would have been obvious to combine Bjorn with Bialick because Bjorn teaches that the USB standard provides for faster transfer of a digitized image. But the discussion in Bjorn about a device having a bus conforming to a USB standard that can receive digital images does not teach or suggest a portable device that has a USB connector that enables the portable device to be coupled directly to a USB socket of another USB-compliant device. Bjorn teaches coupling peripheral devices such as a display, a keyboard, and a mouse to a computer system that has a USB bus (col. 2:64 – col. 3:10), but does not teach or suggest directly coupling a USB plug of a portable device having a non-volatile memory to a USB socket of a USB-compliant device. The memory device of Bjorn is a smart card that has a size and shape similar to a plastic credit card (col. 1:16-18), a form that physically cannot support a USB plug, and Bjorn does not disclose coupling a smart card directly to a USB socket of a USB-compliant device. Thus Bjorn does not teach or disclose the limitation recited in claim 3.

Claim 9 recites a "USB device controller coupled to the bus and a USB plug coupled to the bus, such that the portable data storage device is capable of being coupled directly to a USB socket of . . . a host platform." The Examiner stated that Bialick does not disclose this limitation, but that Bjorn teaches a device with a data bus that conforms to a USB standard (col. 2:59-60) and that it would have been obvious to combine Bjorn with Bialick because

Bjorn teaches that the USB standard provides for faster transfer of a digitized image. But as set forth above regarding claim 3, Bjorn does not disclose a portable device that has a USB connector that enables the portable device to be coupled directly to a USB socket of another USB-compliant device. Further, Bjorn does not disclose a portable device that has a USB plug coupled to a bus of the portable device. Bjorn teaches coupling peripheral devices such as a display, a keyboard, and a mouse to a computer system that has a USB bus (col. 2:64 – col. 3:10), but does not teach or suggest directly coupling a USB plug of a portable device having a non-volatile memory to a USB socket of a USB-compliant device. The memory device of Bjorn is a smart card that has a size and shape similar to a plastic credit card (col. 1:16-18), a form that physically cannot support a USB plug, and Bjorn does not disclose coupling a smart card directly to a USB socket of a USB-compliant device. Also, Bjorn discloses a computer system having a bus, and does not disclose a portable device that has a bus. Thus Bjorn does not teach or disclose the limitation recited in claim 9.

Bialick and Bjorn, either alone or in combination, do not teach or suggest all of the limitations of claims 3 and 9. Thus claims 3 and 9 are not obvious in view of the cited references and are in condition for allowance.

The Examiner rejected claims 23 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Bialick in view of Estakhri. Applicants respectfully traverse.

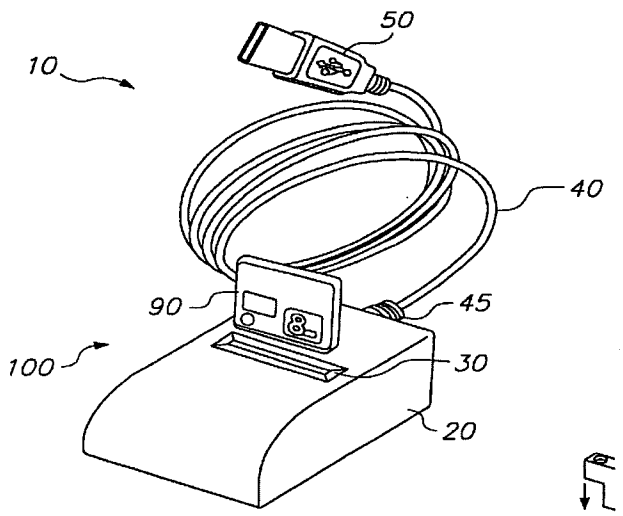
Claim 23 recites a fingerprint module configured to "(1) receive a fingerprint sample from a user placing a finger on the sensor; (2) compare the fingerprint sample with said at least one fingerprint template; and (3) reject a request from the user to access the user data stored in the memory provided that the comparison in said step (2) results in no match." Neither Bialick nor Estakhri discloses this limitation. As set forth above regarding claims 1, 7, and 17, Bialick

does not disclose denying access to a non-volatile memory of a peripheral device unless a biometric authentication is successful. Bialick identifies both storing data and a biometric authentication as target functionalities, and does not teach or disclose any embodiment or mode of operation of the peripheral device in which more than one target functionality is implemented.

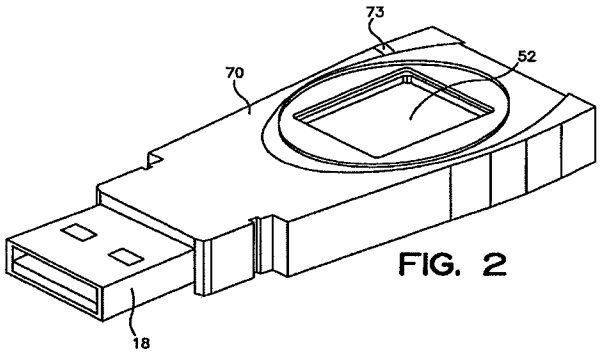
Claim 23 also recites "a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer." The Examiner stated that Estakhri teaches this limitation. But Estakhri does not teach a USB plug integrated into the housing of a portable memory device without an intervening cable. Rather, Estakhri teaches an interface system that has a 50-pin connection as a second end 315 for connection to a removable memory card and has a first end 314 to couple the interface system to a host computer (col. 5, lines 18-44). Estakhri merely teaches that the first end 314 of the interface system is configured for coupling to a host computer system 330 (col. 5, lines 18-20, 45-47), but does not disclose how this coupling is achieved. The first end 314 is for coupling the interface system to a host computer, not for coupling a portable storage device to a host computer.

Estakhri discloses a system that is a combination of a memory card and an interface system with a USB cable. Estakhri's system is not a "unitary portable data storage device." Further, the interface system alone is not a "unitary portable data storage device" as it is an interface for a compact flash card that stores data. In a prior art embodiment where an interface system supports a USB plug, Estakhri discloses that the USB plug 50 is connected to the housing 20 via a cable 40, as clearly shown in Figure 1A of Estakhri, reproduced below. The removable memory card of Estakhri has a 50-pin connection, and does not have a USB plug integrated into its housing. Estakhri does not teach or disclose a USB plug that is integrated into the housing of

a portable data storage device without an intervening cable as recited in claim 23 and as shown in Figure 2 of Applicants' application, reproduced below.



***Estakhri*, Figure 1A**



Applicants' Patent Application, Figure 2

It would not have been obvious to a skilled artisan at the time of the invention to combine Bialick and Estakhri because the combination of Bialick and Estakhri does not disclose all of the limitations of claim 23, and the two references disclose systems geared towards completely opposite objectives. Bialick teaches an access control system that serves to restrict access to

information stored in a host computer, whereas Estakhri teaches an interfacing system that facilitates access to information stored in multiple memory cards. Thus, Bialick and Estakhri teach two distinct endeavors that seek to achieve opposite results: restricting access to stored information in a host computer versus facilitating access to stored information in multiple memory devices. The fact that Bialick and Estakhri refer to flash memory and Estakhri refers to the USB protocol does not, without more, make the two references combinable, and the combination of the two references does not disclose all of the limitations of claim 23. As a result, a skilled artisan would not seek to combine the teachings in Bialick and Estakhri.

Bialick and Estakhri, either alone or in combination, do not teach or disclose all of the limitations of claim 23. Claim 23 is not obvious in view of the cited references and is in condition for allowance.

Claim 24 depends from claim 23, and is allowable for at least the same reasons. Further, claim 24 recites that "at least a portion of the USB plug protrudes from the housing to facilitate direct coupling of the unitary portable storage device to the USB socket." The Examiner stated that Estakhri discloses this limitation. But as set forth above regarding claim 23, Estakhri does not disclose a USB plug integrated into the housing of a portable storage device, so Estakhri cannot disclose that at least a portion of a USB plug integrated into the housing of a portable storage device protrudes from the housing. Bialick and Estakhri, either alone or in combination, do not disclose all of the limitations of claim 24. Claim 24 is not obvious in view of the cited references and is in condition for allowance.

Conclusion

Based on the foregoing amendments and remarks, Applicants respectfully submit that all pending claims in the present application are in condition for allowance and respectfully request

the issuance of a Notice of Allowance. If a telephone conference would facilitate the prosecution of this application, the Examiner is invited to contact Applicants' attorney at the number listed below.

Respectfully submitted,

Dated: December 5, 2011

By: /Wendi R. Schepler/

Wendi R. Schepler
Reg. No. 43,091
Customer No. 007470
WHITE & CASE LLP
(650) 213-0300